REMARKS

The Examiner has rejected all of pending claims 1-18 as anticipated by Bellare. Applicants respectfully traverse this rejection and beg for reconsideration in the light of the remarks that follow.

The present invention, as represented by claim 1, can achieve efficiency in processing a message for authentication. Specifically, the message to be authenticated is provided as an input for processing. If the message fits within an input block of a compression function, the message is processed by a single iteration of the compression function, using a key as a further input. However, if the message does not fit within such an input block, the processing is carried out using a nested hash function. More specifically, the processing is by way of a hash function nested within a keyed hash function.

The Examiner has cited Bellare as disclosing all features of the invention as recited in claim 1. Applicant respectfully disagrees. Bellare does not provide any teaching or suggestion to process the message by alternative procedures, depending on the size of the message relative to an input block. Much less, then, does Bellare provide any teaching or suggestion that one of the alternative procedures should involve a single iteration, whereas the other alternative procedure should involve nested functions.

Accordingly, Applicant respectfully submits that claim 1 and its dependent claims 2-6 are patentable over Bellare under the standards of 35 USC §§ 102(b) and 103. Apparatus claims 14 and 15 are directed to essentially the same invention as method claims 1-6. Therefore, for substantially the same reasons, Applicant submits that claims 14 and 15 meet the same standards for patentability.

The Examiner has cited Bellare, pages 7-9, as disclosing all of the features recited in claim 7. Applicants respectfully disagree. At most, the cited portion of Bellare discusses keyed and iterated hash constructions generally. However, Bellare does not teach, or even suggest, the specific strategy of hashing only one portion of the message,

and then providing both portions of the message as inputs to a hash function, much less a keyed hash function.

According to the method of independent claim 7, on the other hand, the message to be processed has at least two portions, and it is processed by performing at least two hash functions. Specifically, the first portion of the message is hashed to provide an output which for convenience is here denominated RESULT. Then, the second portion of the message and RESULT are used together as inputs to a keyed hash function.

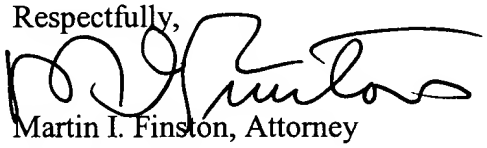
Accordingly, Applicant respectfully submits that claim 7 and its dependent claims 8-13 are patentable over Bellare under the standards of 35 USC §§ 102(b) and 103. Apparatus claims 16-18 are directed to essentially the same invention as method claims 7-13. Therefore, for substantially the same reasons, Applicant submits that claims 16-18 meet the same standards for patentability.

Having responded to all points of rejection, Applicant respectfully solicits allowance of all claims pending in the application.

The Examiner has cited Preneel (U.S. Patent No. 5664016) as prior art made of record and not relied upon, but as considered pertinent to Applicant's disclosure. In the rejection of certain specific claims on page 3 of the Office Action, the Examiner referred to pages 7-9, 16, section 1.1 at page 3, and section 6 at page 15, of "Preneel." It is Applicants' understanding that the cited pages and sections are actually from the Bellare reference. Applicants have responded accordingly.

In view of the foregoing remarks, passage to issue of the subject application is respectfully requested. If the Examiner should feel that the application is not yet in a condition for allowance and that a telephone interview would be useful, he is invited to contact applicants' undersigned attorney at 973, 386-3147.

Respectfully,



Martin I. Finston, Attorney
Reg. No. 31613
973-386-3147

Date: November 8, 2004

Docket Administrator (Room 3J-219)
Lucent Technologies Inc.
101 Crawfords Corner Road
Holmdel, NJ 07733-3030